Procédure et méthodes d'investigation sur Internet

Forget, Catherine

Published in:
L'Europe des droits de l'homme à l'heure d'Internet

Publication date:
2019

Document Version
le PDF de l'éditeur

CHAPITRE 19. PROCÉDURE ET MÉTHODES D'INVESTIGATION SUR INTERNET

Catherine FORGET
Avocate au Barreau de Bruxelles (Jus Cogens)
Chercheuse au CRIDS (UNamur)

I. Introduction

Les méthodes d'enquête entraînent une ingérence dans le droit au respect de la vie privée et dans le droit à la protection des données à caractère personnel garantis par l'article 8 de la Convention européenne des droits de l'homme (ci-après CEDH)[1] et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (ci-après Charte)[2]. Si le choix entre ces différentes techniques relève essentiellement du pouvoir discrétionnaire des États, ceux-ci ne disposent pas pour autant, d'une latitude illimitée[3]. En vertu des articles 8, paragraphe 2, de la CEDH et 52, paragraphe 1, de la Charte, la procédure applicable doit s'inscrire dans le respect des critères de légalité, nécessité et proportionnalité en vue de se prémunir contre le risque d'ingérences illicites ou arbitraires des pouvoirs publics.

Le critère de légalité exige une réglementation « claire, prévisible et accessible » assurant une protection contre les risques d'abus et d'arbitraire[4] et permettant au justiciable, si besoin en s'entourant de conseils éclairés, de régler sa conduite[5]. Le critère de nécessité s'examine à la

1 L'art. 8, § 1, de la CEDH au terme d'une jurisprudence abondante, garantit le droit à la protection des données à caractère personnel mais aussi, sous le couvert du droit à la correspondance, le droit à la confidentialité des communications électroniques. Voy. Cour eur. D.H., 3 avril 2007, n° 62617/00, *Copland c. Royaume-Uni*. En effet, dans l'interprétation de l'art. 8 de la CEDH, est prise en compte la Convention 108 du Conseil de l'Europe, seul instrument contraignant en matière de protection de données au niveau mondial (Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STCE n° 108, 1981). Voy. Cour eur. D.H., 4 mai 2000, n° 27798/5, *Amann c. Suisse*, § 65.

2 La Charte distingue expressément les deux dispositions encadrant dès lors tout traitement de données à caractère personnel indépendamment d'une atteinte éventuelle à la vie privée. C. DOCKSEY, « Articles 7 and 8 of the EU Charter : Two Distinct Fundamental Rights », in *Quelle protection des données personnelles en Europe ?*, Bruxelles, Larcier, 2015, pp. 71-97.

3 Cour eur. D.H., *Gerhard Klass e.a. c. Allemagne*, *Série A*., vol. 28, § 49.

4 Cour eur. D.H., 2 août 1984, *Malone c. Royaume-Uni*, *série A*, n° 82, § 67.

5 Cour eur. D.H., 14 septembre 2010, n° 38224/03, *Sanoma Uitgevers B.V. c. Pays-Bas*, § 81.

lumière des garanties offertes par la disposition tout en tenant compte de la marge d'appréciation laissée aux États membres[6]. Le critère de proportionnalité impose une mesure apte à réaliser l'objectif poursuivi, ne dépassant pas les limites de ce qui est approprié et nécessaire à la réalisation de cet objectif[7].

De manière spécifique, au niveau du Conseil de l'Europe, la Convention sur la cybercriminalité ou Convention de Budapest[8] offre aux États parties un cadre contraignant en matière de procédure pénale[9]. À cette fin, elle exige le respect du principe de proportionnalité[10] mais aussi, lorsque cela s'avère approprié, le respect de conditions et sauvegardes telles une supervision par une juridiction ou un autre organe indépendant, l'indication des motifs justifiant l'exécution de la mesure et la limitation de sa portée ou de sa durée[11]. Au niveau de l'Union européenne, la recommandation n° R (95) 13 offre un cadre non contraignant cette fois et formule des recommandations relatives à certaines méthodes d'enquête[12]. Notons également la directive 2016/680 relative à la protection des données dans les secteurs de la police et de la justice récemment adoptée[13]. Celle-ci encadre le traitement de données par les autorités compétentes notamment à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière[14]. En vue de protéger les droits des personnes concernées, elle impose le respect de mesures techniques et organisationnelles appropriées telles la minimisation des données[15] ainsi que la journalisation pour certaines opérations effectuées à l'aide de systèmes de traitements automatisés[16].

6 Groupe Article 29, avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, 10 avril 2014, pp. 8 et s. Le Groupe de travail de l'Article 29 est institué par la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont précisées à l'art. 30 de la directive 95/46/CE et à l'art. 15 de la directive 2002/58/CE.

7 C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 et C-594/12, §§ 46, 65 et 69.

8 Convention sur la cybercriminalité, signée à Budapest, le 23 novembre 2001, *S.T.C.E.*, n° 185.

9 Art. 16 à 21 de la Convention sur la cybercriminalité.

10 *Ibid.*, art. 15, § 1.

11 *Ibid.*, art. 15, § 2.

12 Recommandation n° R (95) 13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, 11 septembre 1995.

13 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (ci-après directive (UE) 2016/680).

14 Art. 1, § 1, de la directive (UE) 2016/680.

15 *Ibid.*, art. 20.

16 *Ibid.*, art. 25. Ainsi, selon cet article, des journaux devraient être établis dans le cas de la « collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement ».

Dans le cadre de cette contribution, nous exposerons successivement certaines méthodes d'enquête entraînant une ingérence dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel à savoir : l'obligation de conservation de données[17], la préservation de données[18], la saisie de données informatiques[19], le blocage de sites internet[20], l'obligation de collaboration[21] et l'interception des communications[22]. La Cour européenne des droits de l'homme (ci-après Cour eur. D.H.) et la Cour de justice de l'Union européenne (ci-après C.J.U.E.) reconnaissant généralement sans difficulté le caractère légitime de l'objectif poursuivi, à savoir la sécurité nationale[23], nous tâcherons d'identifier directement les garanties minimales dégagées au fil de leur jurisprudence permettant de s'assurer que la mesure est conforme aux droits et libertés fondamentales.

Il est important de noter que la jurisprudence analysée ci-après, revêt une portée limitée. En effet, l'examen d'une technique d'enquête dépend de toutes les circonstances de l'espèce, notamment de : « la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne »[24]. En conséquence, le contrôle effectué dépendra également du système autour duquel s'articule la procédure pénale qu'elle soit accusatoire ou inquisitoire[25].

Dès lors, si cela s'avère nécessaire, nous contextualiserons notre propos en faisant référence à la phase préliminaire de la procédure pénale belge laquelle est dite « inquisitoire » c'est-à-dire secrète, unilatérale et écrite[26]. Sous réserve du flagrant délit[27] et sans préjudice de la mini-instruction[28],

17 C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 et C-594/12 et C.J.U.E., 21 décembre 2016, *Tele 2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department c. Tom Watson e.a.*, aff. jointes C-203/15 et C-698/15 (ci-après arrêt *Tele 2*).

18 § 108 de l'arrêt *Tele 2*.

19 Cour eur. D.H., 2 avril 2014, n^{os} 63629/10 et 60567/10, *Vinci construction et GMT Génie Civil et services c. France*, § 63.

20 Cour eur. D.H., 18 décembre 2012, n° 3111/10, *Ahmet Yildirim c. Turquie*.

21 En matière fiscale par exemple, voy. Cour eur. D.H., 14 mars 2013, n° 24117/08, *Bernh Larsen Holding As c. Norvège*.

22 Cour eur. D.H., 6 septembre 1978, *Gerhard Klass e.a. c. Allemagne*, *Série A*., vol. 28.

23 Cour eur. D.H. (division de la recherche), *Sécurité nationale et jurisprudence de la Cour européenne des droits de l'Homme*, Strasbourg, Conseil de l'Europe, 2013.

24 Cour eur. D.H., 6 septembre 1978, *Gerhard Klass e.a. c. Allemagne*, *Série A*., vol. 28, § 41.

25 M. GIANCLAUDIO et P. DE HERT, « European Human Rights, Criminal Surveillance, and Intelligence Surveillance : Towards Good Enough Judicial Oversight », *Brussels Privacy Hub. Working Paper*, mars 2017, vol. 3, n° 9.

26 A. JACOBS, « Petit tour du monde du contradictoire », in *Le contradictoire dans le procès pénal : nouvelles perspectives* (C. RIBEYRE dir.), Paris, Cujas, 2012, p. 26.

27 Art. 41 et 59 du Code d'instruction criminelle (ci-après « CICr »).

28 Art. 28*septies* CICr.

seul le juge d'instruction est habilité à poser un acte de contrainte susceptible de porter atteinte aux droits et libertés individuelles[29]. En effet, celui-ci instruit à charge et à décharge de manière « indépendante et impartiale » alors que le procureur du Roi assume « le rôle de la partie poursuivante » dans le cadre de l'information[30] et « ne peut donc être considéré comme impartial »[31].

Nous verrons *in fine* que, sans constituer des conditions *sine qua non*, certaines garanties semblent constituer des standards minimums telles l'existence d'une autorisation préalable par un organe indépendant assurant la séparation des pouvoirs ou encore le droit à un recours effectif protégeant les droits de la défense.

II. L'obligation de conservation « généralisée » de données

L'obligation de conservation « généralisée » des « métadonnées »[32] consiste dans la collecte et le stockage systématique et *a priori* de l'ensemble des données traitées et générées lors d'une communication électronique à l'exception du contenu de celle-ci. Ces données conservées par des opérateurs doivent être rendues accessibles sur demande des autorités. Cette méthode implique donc une ingérence « particulièrement grave » dans le droit au respect de la vie privée et à la protection des données à caractère personnel[33].

Cette mesure communément intitulée « rétention de données », est contestable en ce qu'elle implique une délégation d'une mission publique à des acteurs privés. Pour cette raison, le Groupe de l'Article 29 estime celle-ci disproportionnée et recommande d'aligner la durée de conservation de données relatives au trafic sur celle nécessaire au consommateur

29 *Ibid.*, art. 28*bis*, § 3.
30 *Ibid.*, art. 28*bis*.
31 Cons. const., 25 janvier 2017, arrêt n° 6/2017, C 6325 et 6326, B. 5.2.
32 Comme le soulignait déjà à l'époque Yves Poullet, les métadonnées « comprennent outre les données de simple connexion, leur durée, les destinataires de nos messages, les sites visités, la longueur des messages échangés, les caractéristiques du message et du système d'information de l'utilisateur ; les données de localisation révèlent à quelques mètres près l'endroit où se trouvent un mobilophone ou un G.P.S. même non en cours d'utilisation. C'est que l'utilisation de plus en plus intensive des technologies de l'information et la multiplication de services à valeur ajoutée qui leur sont attachées, trahissent les relations que nous nouons avec autrui, nos déplacements, nos goûts, nos convictions voire nos maladies, elles laissent en effet chez des intervenants de plus en plus nombreux et divers, des traces de plus en plus nombreuses en des lieux certes disparates mais certes susceptibles d'être reliés grâce aux vertus des réseaux et de systèmes de plus en plus performants de traitement de l'information », Y. POULLET, « Lutte contre le crime et/ou vie privée : un débat difficile ! À propos de l'alinéa 1er du paragraphe 2 de l'article 109*ter* de la loi belge du 25 mars 1991 introduit par la loi belge du 28 novembre 2000 sur la criminalité informatique », *Terminal*, 2003, p. 42.
33 C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 et C-594/12, § 37.

pour contester la facturation[34]. Cette approche ne fut pas suivie et, dans un contexte marqué par les attentats de Madrid et de Londres en 2004 et 2005, la directive 2006/24/CE[35] fut adoptée. Celle-ci imposait de prévoir à l'égard des opérateurs télécom[36] une obligation de conservation généralisée des données à des fins de lutte contre les infractions graves et le terrorisme. La Cour de justice fut saisie et le 8 avril 2014, dans le cadre de l'arrêt *Digital Rights*, elle invalida la directive 2006/24/CE en raison de l'absence de garanties suffisantes permettant de limiter l'ingérence « au strict nécessaire »[37].

Dans la foulée, la C.J.U.E. fut saisie de deux questions préjudicielles relatives à une règlementation nationale imposant la conservation de données telle que le prévoyait la directive 2006/24/CE[38]. L'arrêt *Tele 2* du 21 décembre 2016 fut l'occasion pour la Cour de préciser sa position. S'alignant sur l'arrêt *Digital Rights*, la Cour caractérisa l'ingérence de « particulièrement grave » et de « vaste ampleur » dans l'exercice du droit à la vie privée et du droit à la protection des données à caractère personnel[39]. Le contrôle devait donc s'opérer de manière « stricte »[40]. Ensuite, la Cour releva le caractère « généralisé et indifférencié » d'un tel dispositif et l'absence de différenciation, limitation ou exception en fonction de l'objectif poursuivi[41]. Partant, la Cour considéra qu'une telle règlementation « excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique » au regard des dispositions dont elle assure le contrôle[42].

Après avoir condamné la conservation généralisée des métadonnées, la Cour précisa les conditions d'une conservation « ciblée » de données appliquée à titre préventif[43]. Selon elle, la règlementation doit indiquer les circonstances et les conditions justifiant de procéder à la conservation

34 Groupe de l'Article 29, recommandation 3/99 relative à la préservation des données de trafic par les fournisseurs de services internet pour le respect du droit, 7 septembre 1999, p. 7.

35 Directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, *J.O.U.E.*, L 105, 13 avril 2006, pp. 54-63, (ci-après directive 2006/24/CE).

36 Les opérateurs télécom sont les opérateurs de « réseaux de communications électroniques » classiques (Orange, Proximus…) et les fournisseurs d'accès à Internet.

37 C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 et C-594/12, § 39 (ci-après arrêt *Digital Rights*).

38 C.J.U.E., 21 décembre 2016, *Tele 2 Sverige AB c. Post-och telestyrelsen* et *Secretary of State for the Home Department c. Tom Watson e.a.*, aff. jointes C-203/15 et C-698/15 (ci-après arrêt *Tele 2*). Pour un commentaire voy. C. FORGET, « L'obligation de conservation des "métadonnnées" : la fin d'une longue saga juridique ? », *J.T.*, 2017, pp. 233-239.

39 § 100 de l'arrêt *Tele 2*.

40 *Ibid.*, § 96.

41 *Ibid.*, § 105.

42 *Ibid.*, § 107.

43 *Ibid.*, § 108.

de données[44], délimiter effectivement l'ampleur de la mesure et, par la suite, viser le « public concerné » par celle-ci[45]. Autrement dit, les données conservées doivent être « susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique »[46].

Par ailleurs, la Cour précisa également les conditions d'accès aux données, à savoir : être soumis à l'autorisation d'une autorité judiciaire ou indépendante[47] à des fins de poursuites relatives à la criminalité grave[48] et à l'égard de personnes liées à l'existence d'une infraction, sauf dans des situations particulières telles la menace d'actes terroristes[49]. En outre, selon la Cour, il est nécessaire d'encadrer la sécurité et protection des données, d'imposer leur conservation sur le territoire de l'Union ainsi que leur destruction à la fin de la période de conservation[50]. Enfin, la mesure devrait être notifiée aux intéressés et être soumise à un contrôle du respect des droits garantis par la Charte[51]. Ce faisant, la Cour précise autant de conditions susceptibles d'être appliquées dans le cas où les autorités souhaiteraient accéder aux données déjà conservées, à des fins de facturation par exemple.

III. La préservation de données

La « préservation de données » encore appelée « gel rapide de données » préconisée par la Convention de Budapest[52] est traditionnellement présentée comme mesure alternative à l'obligation de rétention de données exposée *supra*. Celle-ci serait en effet tout aussi efficace pour lutter contre la criminalité sans pour autant engendrer une ingérence aussi grave dans l'exercice du droit à la vie privée[53]. Cette mesure consiste

44 *Ibid.*, § 109.
45 *Ibid.*, § 110.
46 *Ibid.*, § 111.
47 *Ibid.*, § 120.
48 *Ibid.*, § 115.
49 *Ibid.*, § 119.
50 *Ibid.*, § 122.
51 *Ibid.*, § 123.
52 Art. 16 de la Convention de Budapest.
53 Groupe Article 29, avis 9/2004 sur le projet de décision cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme, 9 novembre 2004 ; CEPD, avis du 26 septembre 2005 sur la proposition de la Commission, pt 77. Le Contrôleur européen pour la protection des données se définit comme « une autorité de contrôle indépendante, qui veille à ce que les

à conserver *a posteriori* et à la suite d'une demande expresse des autorités, certaines données traitées par une personne physique ou morale. Les informations doivent alors être stockées dans les plus brefs délais et ce, pendant une période maximale de nonante jours, ce temps devant permettre aux enquêteurs d'accomplir des formalités supplémentaires[54].

Le rapport explicatif de la Convention de Budapest illustre l'importance de cette technique d'enquête dans le cadre de la lutte contre la criminalité informatique en trois points. En premier lieu, elle permet d'assurer l'intégrité de données volatiles et facilement manipulables tout en ayant des incidences moins importantes pour la réputation d'une entreprise qu'une saisie de données informatiques, par exemple. En second lieu, elle implique la conservation de données de trafic pouvant s'avérer essentielles pour obtenir l'identification de la source de communications et ainsi, l'identité des auteurs d'infractions telle que la diffusion d'images pédopornographiques. En troisième lieu, ce dispositif vise également la conservation des données de contenu susceptibles de révéler que des infractions ont été commises et de servir à titre de preuves[55].

IV. La saisie de données informatiques

Un système informatique autrement dit, un ordinateur, un serveur ou encore un téléphone portable, est protégé par l'article 8 de la Convention européenne des droits de l'homme[56]. Il comprend des données relevant de la vie privée des personnes, par exemple des carnets d'adresses, des photographies, des données professionnelles[57], ou encore des données

institutions et organes communautaires respectent leurs obligations en matière de protection des données. Ces règles sont énoncées dans le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données ».

54 Art. 16 de la Convention sur la cybercriminalité, Budapest, 23 novembre 2001, *S.T.C.E.*, n° 185.

55 Rapport explicatif de la Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001, § 154.

56 À titre illustratif, le considérant 24 de la directive 2002/58/CE précise que : « [l]'équipement terminal de l'utilisateur d'un réseau de communications électroniques ainsi que toute information stockée sur cet équipement relèvent de la vie privée de l'utilisateur, qui doit être protégée au titre de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ». Voy. directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, *J.O.C.E.*, C.E L 201/37, 31 juillet 2002, pp. 0037-0047 (ci-après directive 2002/58/CE).

57 Dans l'arrêt *Niemietz*, la Cour eur. D.H. a expressément inclus les relations professionnelles dans le champ d'application du droit au respect de la vie privée. Elle précise en effet qu'il paraît « n'y avoir aucune raison de principe de considérer cette matière de comprendre la notion de « vie privée » comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur ». Cour eur. D.H., 16 décembre 1992, n° 13710/88, *Niemietz c. la République fédérale d'Allemagne*, § 29.

médicales. Un système informatique est un espace virtuel pouvant être perçu par son utilisateur comme un lieu d'activité « au sein duquel un individu a le sentiment d'être dans l'intimité, en sécurité contre l'immixtion de personnes contre sa volonté, indépendamment de la durée et de l'intensité d'utilisation »[58]. Cette approche rejoint la définition du domicile privé de la Cour européenne des droits de l'homme[59]. L'intrusion dans ce système « privé » pourrait donc *a priori* être perçue comme une mesure de perquisition au sens classique du terme.

En conséquence, selon la recommandation n° R (95) 13 du Conseil de l'Europe[60] et la Convention de Budapest[61], dans le cas d'une intrusion dans un système par des autorités en vue de saisir des données, la procédure applicable dans le contexte numérique devrait s'aligner sur celle prévue « dans le cadre des pouvoirs traditionnels » de perquisition et de saisie. La personne devrait être informée de la « perquisition et de la nature des données saisies » et disposer à cet égard de « recours juridiques »[62].

Précisons que par « perquisition », il y a lieu d'entendre « rechercher, lire, inspecter ou examiner des données »[63] tandis que la « saisie de données informatique » vise le fait de prendre possession des données, de les copier, de les rendre inaccessibles ou de les retirer du système indépendamment de la soustraction du support[64]. L'emploi du mot « perquisitionner » traduit donc « l'idée de l'exercice par l'État d'un pouvoir coercitif et montre que le pouvoir visé dans cet article est analogue à la perquisition classique »[65]. Dès lors, pour obtenir l'autorisation de procéder à une mesure de perquisition, il faut disposer de raisons de penser que de telles données « existent dans un endroit précis et permettent de prouver qu'une infraction pénale spécifique a été commise »[66]. Par contre, à la différence d'une perquisition classique, la Convention de Budapest n'exige pas d'informer les parties intéressées

58 *Ibid.*, *Rev. trim. D.H.*, 1993, p. 467 et *J.T.*, 1994, p. 65, note E. JAKHIAN et P. LAMBERT, « Les perquisitions dans les cabinets d'avocat ».

59 Voy. not. Cour eur. D.H., 16 avril 2002, n° 37971/97, *Société Colas Est et autres c. France*, § 41 ; Cour eur. D.H, 9 décembre 2004, n° 41872/98, *Van Rossem c. Belgique*.

60 Recommandation n° R (95) 13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, 11 septembre 1995, § 2.

61 Rapport explicatif de la Convention sur la cybercriminalité, § 191.

62 Recommandation n° R (95) 13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, 11 septembre 1995, § 2.

63 Rapport explicatif de la Convention sur la cybercriminalité, § 191.

64 Art. 19, § 4, de la Convention sur la cybercriminalité.

65 Rapport explicatif de la Convention sur la cybercriminalité, § 191.

66 *Ibid.*, §§ 185-186.

du déclenchement de la procédure considérant qu'une telle notification pourrait nuire au bon déroulement de l'enquête[67].

En Belgique, avant l'adoption de la loi du 25 décembre 2016[68], la procédure en vigueur prévoyait une distinction entre la saisie de données informatiques, relevant de la compétence du procureur du Roi, et la recherche ou l'extension de recherche dans un système, relevant de la compétence du juge d'instruction[69]. Ce régime faisait l'objet de controverses, le Code d'instruction criminelle ne précisant pas si les enquêteurs pouvaient exploiter un système informatique sans disposer de l'autorisation d'un juge d'instruction[70]. La question fut tranchée par la Cour de cassation dans un arrêt du 11 février 2015. La Cour dit pour droit que « l'exploitation de la mémoire d'un téléphone portable, dont les messages qui y sont stockés sous la forme d'un sms, est une mesure découlant de la saisie, laquelle peut être effectuée dans le cadre d'une information sans autres formalités que celles prévues pour cet acte d'enquête »[71]. Cette jurisprudence fut entérinée par la loi du 25 décembre 2016[72] faisait fi de la nécessité de distinguer la « saisie » de données de la « recherche » dans un système dont la portée de l'ingérence diffère[73].

De son côté, la Cour eur. D.H. fut rarement confrontée à des litiges relatifs à une saisie de données indépendamment d'une perquisition dans un lieu réel opérant dès lors une certaine confusion entre saisie,

67 *Ibid.*, § 204.

68 Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.*, 17 janvier 2017.

69 Art. 39*bis* et 88*ter* CICr.

70 Certains auteurs considéraient par exemple que « [n]e constitue pas une recherche informatique l'exploitation d'un système informatique qui a été légalement saisi et qui se trouve entre les mains des enquêteurs (un smartphone, une tablette, un ordinateur…) » ; O. LEROUX, « Criminalité informatique », in *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, juillet 2014, C 362/46, p. 58.

71 Cass., 11 février 2015, P. 14.1739.F, www.cass.be. Pour un commentaire d'arrêt voy. C. FORGET, « Quelles garanties entourent la saisie de données informatiques et l'exploitation d'un système de données informatiques », *R.D.T.I.*, décembre 2015, n° 61, pp. 79-90 ; C. CONINGS, « Het uitlezen van een gsm of een ander privaat IT-systeem : This is not America », note sous Cass., 11 février 2015, *R.W.*, 2015-2016, pp. 622-626.

72 La loi du 25 décembre 2016 entérine cette jurisprudence et permet désormais à tout officier de police judiciaire d'effectuer une recherche dans un système informatique ou une partie de celui-ci à condition de la saisie du support. Dans l'hypothèse où le système informatique n'est pas saisi mais pourrait l'être, par exemple si l'ordinateur est situé dans un cybercafé ou si l'enquête se déroule dans une banque, l'officier de police judiciaire devra requérir l'autorisation du procureur du Roi avant d'entamer une recherche. En cas d'extrême urgence, ce dernier pourra ordonner la recherche oralement et devra confirmer l'autorisation par écrit dans les meilleurs délais en précisant les motifs de l'extrême urgence. Voy. art. 39*bis*, § 2, al. 2, CICr et 39*bis*, § 3, al. 6, CICr.

73 Nous rejoignons l'analyse de certains auteurs selon laquelle toute recherche dans un système informatique par les autorités devrait être encadrée par les mêmes garanties qu'une mesure de perquisition. C. MEUNIER, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », *Rev. dr. pén.*, 2001/7-8, pp. 663 et 664 ; T. INCALZA, « Strafonderzoek in het digitale tijdperk : zoeking en inbeslagneming », *Jura Falc.*, 2010-2011/2, pp. 329-383.

recherche et perquisition. Il est possible toutefois de tirer certains enseignements de sa jurisprudence.

Dans le cadre d'une recherche dans un système informatique, la règle semble être celle du mandat judiciaire ou de l'autorisation préalable par un organe indépendant[74], à l'instar d'une perquisition classique[75]. Celle-ci doit permettre de s'assurer de l'existence de soupçons raisonnables à l'encontre de l'intéressé justifiant de procéder à la fouille dans un système et ainsi, garantir la séparation des pouvoirs[76]. Ce mandat peut être rédigé en termes larges, la Cour eur. D.H. prenant également en considération « la façon dont la perquisition a été menée, y compris la présence ou non d'observateurs indépendants, et l'étendue des répercussions possibles sur le travail et la réputation de la personne visée par la perquisition »[77]. À titre illustratif, un mandat autorisant une recherche sur base de 35 mots-clés peut s'avérer compatible avec la Convention eu égard aux garanties offertes à l'intéressé pendant la recherche dans le système, en l'occurrence : la présence de l'avocat mis en examen et d'un membre de l'ordre et la rédaction d'un procès-verbal décrivant le déroulement des opérations[78]. Notons qu'en l'espèce, outre la recherche, une saisie fut opérée sur plus de 89.000 fichiers et plus de 29.000 messages électroniques. À cet égard, la Cour releva également les garanties offertes à l'intéressé à savoir : l'interdiction de saisir des documents couverts par le secret professionnel d'un avocat non visé par l'enquête, la mise sous scellés immédiate des documents saisis, le visionnage de ces derniers par un juge d'instruction ainsi que leur suppression s'ils ne sont pas utiles dans le cadre de l'enquête et enfin, la possibilité pour les intéressés d'introduire une réclamation auprès du président de la Cour d'appel avec une mise sous scellés des données sans consultation possible dans l'attente de sa décision.

Quant à la saisie de données informatiques, la Cour ne semble pas exiger de cibler préalablement les données emportées ou copiées pour autant que les intéressés disposent d'un contrôle effectif. Ainsi, dans

74 Sur la notion d'« organe indépendant », voy. *infra*, VII, D, La notification *a posteriori* et le contrôle effectif par un organe indépendant.

75 Voy. par exemple Cour eur. D.H., 9 décembre 2004, n° 41872/98, *Van Rossem c. Belgique*.

76 Comme le souligne le Juge Zupančič, « l'intrusion n'est donc justifiée qu'une fois le soupçon déjà "raisonnable", c'est-à-dire lorsqu'il est très probable que le suspect a déjà enfreint la loi ». Selon ce dernier, le soupçon raisonnable devrait être « *a priori* », « concret », « spécifique » et « articulable » afin de permettre au juge de disposer au préalable d'informations réelles et pas seulement de l'intuition de l'autorité auteur de l'intrusion. Opinion concordante de Juge Zupančič, à laquelle se rallie le Juge De Gaetano, Cour eur. D.H., 2 avril 2014, n° 63629/10, *Vinci construction et GMT Génie Civil et services c. France*, §§ 78 et 79.

77 Cour eur. D.H., 3 septembre 2015, n° 27013/10, *Sérvulo & Associados Advogados rl c. Portugal*, § 100.

78 *Ibid.*, § 103. Voy. Dans le même sens Cour eur. D.H., 16 octobre 2007, n° 74336/01, *Wieser et Bicos Beteiligungen GmbH c. Autriche*.

l'affaire *Vinci* par exemple, la Cour a considéré qu'un inventaire remis aux intéressés *a posteriori* détaillant le nom des fichiers, leur extension, leur provenance, leur empreinte numérique ainsi qu'une copie des documents saisis, constituait une garantie suffisante au regard de l'article 8, paragraphe 2, de la Convention. En effet, selon la Cour, les intéressés étaient en mesure de vérifier que seules les données en lien avec l'objet de l'enquête avaient été emportées de sorte qu'il ne s'agissait pas d'une saisie « massive et indifférenciée » susceptible d'emporter la violation de la Convention[79]. En revanche, une mesure n'organisant pas de recours effectif pourrait emporter la violation de l'article 8 de la CEDH, les personnes concernées ne pouvant mettre en cause la régularité de la saisie et le juge, en contrôler la légalité afin, si nécessaire, d'ordonner la restitution voire l'effacement des documents saisis[80].

En définitive, la recherche dans un système informatique requiert en principe une autorisation préalable par un organe indépendant, sauf exceptions[81]. Cette autorisation permet de s'assurer de l'existence de soupçons raisonnables et d'éviter une « saisie massive et indifférenciée »[82] en référence aux « *fishing expeditions* » c'est-à-dire une fouille effectuée dans l'espoir d'y trouver la preuve d'une infraction[83]. Par contre, la saisie peut être effectuée de manière large pour autant que la procédure offre un recours effectif c'est-à-dire la possibilité de contester la régularité de celle-ci devant un juge et d'obtenir la restitution voire l'effacement des documents saisis[84].

79 Cour eur. D.H., 2 avril 2014, n^os^ 63629/10 et 60567/10, *Vinci construction et GMT Génie Civil et services c. France*, § 76.

80 Cour eur. D.H., 21 mars 2017, n° 33931/12, *Société Janssen Cilag c. France*, § 23 ; Cour eur. D.H., 2 avril 2014, n° 63629/10, *Vinci construction et GMT Génie Civil et services c. France*, § 78.

81 Dans l'arrêt *Trabajo Rueda*, la Cour semble avoir implicitement reconnu qu'une recherche dans un système informatique requiert en principe une autorisation préalable sauf exceptions. Elle précisa en effet : « 35. La Cour constate que, en ce qui concerne l'accès au contenu d'un ordinateur personnel par la police, la jurisprudence du Tribunal constitutionnel a établi la règle de l'autorisation judiciaire préalable, condition exigée en tout état de cause par l'article 8 de la Convention (qui requiert la délivrance d'un mandat par un organe indépendant) lorsqu'une atteinte à la vie privée d'une personne est en jeu. La jurisprudence constitutionnelle espagnole permet toutefois, à titre exceptionnel, de passer outre une telle autorisation dans des situations d'urgence ("nécessité urgente") pouvant faire l'objet d'un contrôle judiciaire postérieur ». Ce contrôle doit permettre de vérifier la réalité de l'urgence c'est-à-dire d'examiner l'existence de raisons pour lesquelles l'attente de cette autorisation risque d'entraver le bon déroulement de l'enquête. En l'espèce, les services de police avaient consulté les données contenues dans un ordinateur portable qui leur avait été remis. La Cour a considéré qu'il était difficile d'apprécier la réalité de l'urgence, la consultation de données informatiques visant les archives d'un système entre les mains des autorités et par ailleurs déconnecté d'Internet (Cour eur. D.H., 30 mai 2017, n° 32600/12, *Trabajo Rueda c. Espagne*, § 35).

82 Cour eur. D.H, 16 octobre 2008, n° 10447/03, *Maschino c. France*, § 34.

83 Opinion concordante de Juge Zupančič, à laquelle se rallie le Juge De Gaetano, Cour eur. D.H., 2 avril 2014, n° 63629/10, *Vinci construction et GMT Génie Civil et services c. France*, §§ 78 et 79.

84 Cour eur. D.H., 21 mars 2017, n° 33931/12, *Société Janssen Cilag c. France*, § 23 ; Cour eur. D.H., 2 avril 2014, n° 63629/10, *Vinci construction et GMT Génie Civil et services c. France*, § 78.

V. Le blocage de sites internet

L'affaire *Pirate Bay* témoigne de l'importance d'encadrer toute mesure visant le blocage de sites internet, celle-ci étant susceptible de mettre à mal tant le droit au respect de la vie privée que le droit à la liberté d'expression. En l'espèce, en vue de faire cesser une violation des droits de la propriété intellectuelle, une ordonnance du juge d'instruction prise sur la base de l'article 39*bis*, paragraphe 4, CICr, soit la saisie de données informatiques, enjoignait aux opérateurs de rendre inaccessible le contenu des sites liés à l'adresse IP du nom de domaine « thepiratebay.org ». Ces derniers devaient effectuer un procédé technique « *reverse IP domain check* » afin de déterminer les noms de domaines renvoyant au serveur lié à « thepiratebay.org » et d'en bloquer l'accès[85]. La Cour de cassation confirma la base légale applicable considérant que le blocage de sites internet découlerait de la saisie de données informatiques, la disposition susmentionnée permettant au procureur du Roi de rendre inaccessibles les données formant l'objet de l'infraction, produites par l'infraction ou contraires à l'ordre public et aux bonnes mœurs ou encore risquant d'endommager un système informatique[86].

Cette interprétation fut vivement critiquée en raison de la nature provisoire et temporaire de la saisie, celle-ci visant à conserver des données à titre de preuve ou pouvant servir à la manifestation de la vérité. Elle ne saurait donc recouvrir un caractère permanent[87]. De plus, si en l'espèce, le blocage de sites internet fut certes souhaité compte tenu de la violation flagrante des droits de propriété intellectuelle, une telle jurisprudence comporte un certain danger. En effet, ce faisant, la Cour de cassation attribue au procureur du Roi une mesure de contrainte susceptible de porter atteinte à la fois à l'exercice du droit au respect de la vie privée et au droit à la liberté d'expression dont l'exercice devrait relever de la compétence du

85 Notons que les demandeurs en cassation contestaient également l'obligation de collaboration qui leur étaient due. Ils invoquaient l'art. 21 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information (actuellement XII.20 du Code de droit économique). En effet, l'art. précité réfère *in fine* à l'art. 39*bis* CICr en précisant que le prestataire *peut* empêcher l'accès aux données, le temps nécessaire au procureur du Roi de prendre des dispositions, par exemple requérir un mandat de perquisition. Ce dernier n'a pas l'obligation de prendre des mesures. La Cour n'a pas retenu cet argument et, se basant sur le § 4 de l'art. 39*bis* CICr, considéra que cette disposition « n'exclut pas que cet ordre soit adressé à des tiers », obligeant dès lors ces derniers à collaborer (Cass. (2e ch., sect. nl.), 22 octobre 2013, P. 13.0550.N, www.cass.be). Pour un commentaire d'arrêt voy. R. SCHOEFS, « Changement de méthode dans la lutte contre The Pirate Bay : la saisie de données autorisée », *T. Strafr.*, 2014/2, pp. 131-142 (note sous Cass., 22 octobre 2013, P. 13.0550.N et P. 13.0551.N) ; P. MONVILLE et M. GIACOMETTI, « Les fournisseurs d'accès à Internet, nouveaux gendarmes de la toile ? », *R.D.T.I.*, 2014/2, n° 55, pp. 68-76.

86 Art. 39*bis*, § 6, CICr.

87 F. LUGENTZ et D. VANDERMEERSCH, « Chapitre 2. Les choses susceptibles d'être saisies », in *Saisie et confiscation en matière pénale*, Bruxelles, Bruylant, 2015, pp. 103-128.

juge d'instruction[88]. Du côté des États membres du Conseil de l'Europe[89], la procédure varie selon le système juridique et le contenu visé. Toutefois, il est possible de dégager certaines pratiques communes. Ainsi, en cas d'urgence dans des matières liées à la pédopornographie ou le terrorisme par exemple, le contenu pourra être bloqué en l'absence d'une autorisation judiciaire préalable, sur décision d'une autorité administrative, des services de police ou du procureur. En outre, la plupart des pays offrent aux personnes intéressées une voie de recours permettant de contester la mesure. Dans les domaines liés à la propriété intellectuelle, à la violation de la vie privée ou à la diffamation, les États exigent généralement une ordonnance judiciaire ou encore permettent d'engager la responsabilité des intermédiaires en tant que tiers en l'absence de leur réaction[90].

La Cour de Strasbourg a développé une jurisprudence abondante sur les responsabilités des hébergeurs et des éditeurs de contenu, analysée dans plusieurs contributions de cet ouvrage. Par contre, dans le domaine spécifique du blocage de sites internet, elle n'a pas encore eu l'occasion de baliser les bonnes pratiques à suivre afin de s'assurer que l'ingérence soit conforme à la CEDH. Notons toutefois que dans le cadre de l'arrêt *Ahmet Yildirim c. Turquie*[91], le Juge Pinto de Albuquerque édicta dans une opinion concordante[92] un ensemble de lignes directrices claires à suivre en la matière, à savoir :

1) une définition des catégories de personnes et d'institutions susceptibles de voir leurs publications bloquées (les propriétaires nationaux ou étrangers de contenus, sites ou plates-formes illicites, les utilisateurs de ces sites ou plates-formes etc.) ;

88 Pour rappel, le juge d'instruction instruit à charge et à décharge et doit être considéré comme indépendant et impartial tandis que le procureur du Roi assume le rôle de la partie poursuivante.

89 Selon une étude du Conseil de l'Europe, « un nombre significatif de pays » ne disposent d'aucun système législatif encadrant les conditions et procédure à respecter permettant de procéder à une mesure de blocage ou de retrait de contenus illégaux véhiculés par Internet. Certains s'appuient sur le secteur privé encourageant la mise en place de code de conduite sur Internet par exemple, d'autres délèguent aux juridictions nationales le soin de veiller à un juste équilibre entre le respect des droits fondamentaux et la sécurité sur Internet, d'autres encore incluent le blocage de site internet dans la saisie de données informatiques. Conseil de l'Europe, *Étude comparative sur le filtrage, le blocage et la suppression de contenus illégaux sur l'Internet*, Strasbourg, Conseil de l'Europe, 2017, p. 12.

90 *Ibid.*, pp. 12 et s.

91 Cour eur. D.H., 18 décembre 2012, n° 3111/10, *Ahmet Yildirim c. Turquie*. La Cour fut saisie d'un litige relatif à une mesure de blocage de site internet. Un tribunal avait ordonné de bloquer l'accès à « Google sites » afin d'empêcher la consultation d'un site internet dont le propriétaire était poursuivi pour outrage à la mémoire d'Atatürk. Le requérant, personne tierce à la procédure, invoquait la violation du droit à la liberté d'expression, celui-ci ne pouvant plus accéder à son propre site internet alors qu'il n'était pas lié aux poursuites pénales entamées. La Cour constata l'absence de base légale suffisante mais aussi l'absence de garanties suffisantes contre les risques d'abus et d'arbitraire.

92 Opinion concordante du Juge Pinto de Albuquerque, Cour eur. D.H., 18 décembre 2012, n° 3111/10, *Ahmet Yildirim c. Turquie*.

2) une définition des catégories d'ordonnances de blocage, par exemple celles qui visent le blocage de sites, d'adresses IP, de ports, de protocoles réseaux, ou le blocage de types d'utilisation, comme les réseaux sociaux ;
3) une disposition sur le champ d'application territorial de l'ordonnance de blocage ;
4) une limite à la durée d'une telle ordonnance de blocage ;
5) l'indication des « intérêts » justifiant la mesure, du critère de proportionnalité et de nécessité ;
6) la détermination des autorités compétentes pour émettre une ordonnance de blocage motivée ;
7) une procédure à suivre pour l'émission de cette ordonnance, comprenant l'examen par l'autorité compétente du dossier à l'appui de la demande d'ordonnance et l'audition de la personne ou institution lésée, sauf si cette audition est impossible ou se heurte aux « intérêts » poursuivis ;
8) la notification de l'ordonnance de blocage et de sa motivation à la personne ou institution lésée ;
9) une procédure de recours de nature judiciaire contre l'ordonnance de blocage.

Ces critères illustrent la nécessité de prévoir des garanties suffisantes et en conséquence, d'encadrer le blocage de sites internet en tant que mesure à part entière et non de l'intégrer dans une mesure préexistante telle la saisie de données informatiques.

VI. L'obligation de collaboration

Les mesures de cryptage permettent d'assurer la protection des données à caractère personnel[93] et en ce sens, contribue à protéger le droit

[93] Différents instruments internationaux préconisent le chiffrement de données en vue d'assurer la sécurité des flux et la protection des données à caractère personnel. L'art. 31, § 1, du Règlement général sur la protection des données liste certaines mesures permettant de garantir un niveau de sécurité informatique adapté dont la première est « le chiffrement des données à caractère personnel ». De même, une recommandation du Comité des ministres du Conseil de l'Europe préconise l'application de mesures de cryptage « de bout en bout » afin d'éviter l'accès illicite aux données par des tiers. Voy. recommandation CM/Rec(2014) 6 du Comité des ministres aux États membres sur un guide des droits de l'homme pour les utilisateurs d'Internet, adoptée par le Comité des ministres le 16 avril 2014 ; dans le même sens, l'Assemblée parlementaire du Conseil de l'Europe affirme qu'un « cryptage généralisé destiné à renforcer le respect de

au respect de la vie privée[94]. Toutefois, selon la Convention de Budapest, les autorités répressives se heurtant à des données chiffrées[95] peuvent imposer la collaboration de tiers afin d'obtenir les données en leur possession ou sous leur contrôle[96] en « texte clair »[97], c'est-à-dire déchiffrées. Considérant qu'il s'agit d'une méthode d'enquête, elle exige le respect du critère de proportionnalité mais aussi de prendre en considération l'intérêt légitime de tiers[98].

À ce propos, l'affaire *Apple* défraya la chronique en raison du refus de l'entreprise d'obtempérer à une injonction du FBI lui ordonnant de déchiffrer le téléphone portable d'un des auteurs de la tuerie de San Bernardino. Outre le déblocage du téléphone, le FBI souhaitait qu'Apple élabore une nouvelle version du système d'exploitation afin de faciliter de manière générale l'accès des autorités aux données stockées sur ses appareils, indépendamment de celui visé dans le cadre de l'enquête. Apple refusa d'agir invoquant le risque de mettre à mal la sécurité informatique de ses services en installant un tel logiciel. *In fine*, le FBI trouva une faille et accéda aux données contenues sur le téléphone sans la collaboration de la multinationale laissant en suspens la problématique du refus de collaboration d'un tiers en cas de chiffrement des données.

Au niveau des instances internationales, le rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression des Nations unies estime qu'une obligation de collaboration est une ingérence qui devrait « être strictement limitée, conformément aux principes de légalité, de nécessité, de proportionnalité et de légitimité des objectifs »[99]. Selon ce dernier, les États devraient « éviter toutes les

la vie privée reste la riposte la plus efficace pour permettre aux citoyens de protéger leurs données », voy. rapport de la commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe, Rapporteur M. Pieter Omtzigt, doc. 13734 du 18 mars 2015, pt 119.

94 Ce lien de dépendance a été illustré dans l'arrêt *I. c. Finlande* où la Cour eur. D.H. estima que le défaut de garanties relatives à la sécurisation des données contre des usages non-autorisés constitue une violation de l'obligation positive d'assurer le respect du droit à la vie privée consacré à l'art. 8 de la CEDH. Cour eur. D.H., 17 juillet 2008, n° 20511/03, *I. c. Finlande*.

95 Europol affirme que le chiffrement des données ralentit considérablement la poursuite des enquêtes pénales. Europol, « The Internet Organised Crime Threat Assessment (IOCTA) 2015 », 30 septembre 2015, pp. 67 et s.

96 L'expression « en sa possession » ou « sous son contrôle » fait référence d'une part, à la possession matérielle des données et d'autre part, à des situations dans lesquelles l'intéressé ne possède pas matériellement les données à produire mais peut en contrôler librement la production, par exemple si les données sont stockées sur un *cloud* qu'il met librement à disposition. Le rapport explicatif précise toutefois qu'un accès aux données par une liaison du réseau ne constitue pas nécessairement un « contrôle » au sens de la présente disposition. Rapport explicatif de la Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001, § 173.

97 Rapport explicatif de la Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001, § 176.

98 Art. 18, § 2, de la Convention de Budapest.

99 Rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, A/HRC/29/32, 22 mai 2015, § 56.

mesures qui affaiblissent la sécurité en ligne des individus, telles que des portes dérobées, de faibles standards de cryptographie ou la rétention de clés de chiffrement »[100]. Dans le même sens, la recommandation n° R (95) 13 du Comité des ministres aux États membres du Conseil de l'Europe relative aux problèmes de procédure pénale liés à la technologie de l'information dispose : « des mesures devraient être examinées afin de minimiser les effets négatifs de l'utilisation du chiffrement sur les enquêtes des infractions pénales, sans toutefois avoir des conséquences plus que strictement nécessaires sur son utilisation légale »[101].

La Cour eur. D.H. n'a pas été amenée à se prononcer sur la question mais a été saisie d'un litige relatif à la collaboration de tiers en raison de l'anonymat d'internautes. À cette occasion, elle a déduit du droit au respect de la vie privée une obligation positive pour les États membres de prévoir dans leur droit interne des dispositions permettant d'exiger d'un fournisseur de service internet de dévoiler l'identité d'un destinataire de leurs services[102]. La C.J.U.E. adopte une position similaire dans le domaine de la propriété intellectuelle en reconnaissant que des acteurs privés puissent être tenus de sécuriser une connexion internet et d'imposer à l'utilisateur de s'identifier[103].

On précisera encore que l'obligation de collaboration ne pourrait porter atteinte au droit au silence garanti par l'article 6, paragraphe 3, de la CEDH. En Belgique, par exemple, en vertu de l'article 88*quater*, paragraphe 1 du Code d'instruction criminelle, toute personne présumée disposer d'une connaissance particulière du système informatique peut être tenue, sur ordonnance du juge d'instruction, de fournir des informations sur le fonctionnement de ce système sous peine de sanctions pénales[104]. Le tribunal correctionnel de Termonde a toutefois rappelé qu'aucun suspect ne peut être obligé de collaborer activement avec les autorités poursuivantes. Il estima qu'en ordonnant aux prévenus de rendre accessibles les supports de données, ces derniers avaient été contraints, moyennant une prestation intellectuelle propre, de contribuer activement à

100 *Ibid.*, § 60.

101 Recommandation n° R (95) 13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, 11 septembre 1995, § 14.

102 Cour eur. D.H., 2 décembre 2008, n° 2872/02, *K.U. c. Finlande*, § 49. Selon celle-ci, « [m]ême si la liberté d'expression et la confidentialité des communications sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, cette garantie ne peut être absolue, et elle doit parfois s'effacer devant d'autres impératifs légitimes tels que la défense de l'ordre et la prévention des infractions pénales ou la protection des droits et libertés d'autrui ».

103 C.J.U.E., 15 septembre 2016, *Tobias Mc Fadden c. Sony Music Entertainment Germany GmbH*, C-484/14.

104 Art. 88*quater*, § 3, CICr.

l'administration de la preuve à leur encontre de sorte que les éléments de preuve fournis par les supports de données cryptées étaient frappés de nullité[105]. Cette approche fut confirmée par la Cour d'appel de Gand[106]. Récemment toutefois, la Cour d'appel d'Anvers, chambre des mises en accusation, a considéré que l'ordonnance d'un juge d'instruction imposant à un inculpé de dévoiler le code PIN de son téléphone portable afin de permettre aux enquêteurs d'exploiter les données stockées, n'était pas incompatible avec les exigences du droit à un procès équitable[107]. La chambre des mises en accusation s'est notamment basée sur l'arrêt *Saunders* de la Cour eur. D.H. Dans cette décision, la Cour eur. D.H. a estimé qu'une donnée que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais existant indépendamment de la volonté d'un suspect, telles des documents recueillis sur la base d'un mandat, des empreintes ADN, haleine, sang, urine, n'entrent pas dans le champ d'application du droit au silence[108]. Cette interprétation mérite d'être nuancée puisqu'à la différence de documents fiscaux tenus en vertu d'une obligation légale par exemple, un mot de passe est créé sur initiative de son auteur et devrait donc être couvert par le droit au silence[109].

VII. L'interception des communications

Selon l'article 21 de la Convention de Budapest, un dispositif d'interception des communications est considéré comme particulièrement intrusif et doit être limité aux enquêtes relatives à « un éventail d'infractions graves à définir en droit interne »[110]. Le rapport explicatif complète cette disposition en exigeant un ensemble de conditions et de sauvegardes spécifiques, à savoir : une supervision judiciaire ou un autre mode de supervision indépendante, l'indication des communications à intercepter ou des personnes concernées, la limitation de la durée de l'interception, la motivation de la mesure au regard du respect des principes de nécessité, subsidiarité et proportionnalité et enfin, l'existence d'un droit de recours[111].

105 Corr. Termonde, 17 novembre 2014.
106 Gand, 23 juin 2015, *NjW*, 2016, liv. 336, p. 134, note C. CONINGS.
107 Anvers (ch. des mises en accusation), 21 décembre 2017, K/2895/2017, inédit.
108 Cour eur. D.H., 17 décembre 1996, n° 1187/91, *Saunders c. Royaume-Uni*, § 69.
109 Cour eur. D.H., 25 février 1993, n° 110588/83, *Funke c. France*.
110 Art. 21, § 1, de la Convention de Budapest.
111 Rapport explicatif de la Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 novembre 2001, § 215.

Dans l'arrêt *Schrems*, la Cour de justice de l'Union européenne a fermement condamné toute mesure permettant l'interception *généralisée* du contenu des communications, celle-ci impliquant une « atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte »[112]. De son côté, la Cour eur. D.H. a été saisie à de nombreuses reprises de recours exercés tant par des particuliers que par des associations de défenses des droits de l'homme[113].

Dans le domaine des mesures de surveillance secrète[114], la Cour eur. D.H. tient compte des critères suivants : « la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer

112 C.J.U.E. (Gde ch.), 6 octobre 2015, *Maximilian Schrems c. Data Protection Commissioner*, C-362/14. Cette affaire fait suite à une plainte de Monsieur Schrems visant à faire interdire le transfert de ses données par Facebook Ireland vers les États-Unis. Celui-ci s'appuyant sur les révélations d'Edward Snowden, dénonçait l'absence de niveau de protection adéquat des données à caractère personnel sur le sol américain en dépit de la décision *Safe Harbor* de la Commission

113 En effet, cette mesure ayant pour particularité de s'exercer à l'insu des intéressés implique une appréciation plus souple par la Cour de la qualité de « victime ». Premièrement, celle-ci tient compte de l'ensemble des circonstances de la cause notamment de la portée de la législation et de la situation individuelle du requérant. Celui-ci peut dès lors s'estimer concerné « soit parce qu'il appartient à un groupe de personnes visées par elle, soit parce qu'elle concerne directement l'ensemble des usagers des services de communication en instaurant un système dans lequel tout un chacun peut voir intercepter ses communications ». Deuxièmement, la Cour tient compte de l'existence d'un droit de recours offert à toute personne présumant faire l'objet d'une mesure d'interception, et de l'effectivité de celui-ci. En effet, « lorsque l'ordre interne n'offre pas de recours effectif à la personne qui pense avoir fait l'objet d'une surveillance secrète, les soupçons et les craintes de la population quant à l'usage abusif qui pourrait être fait des pouvoirs de surveillance secrète ne sont pas injustifiés » (Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 171). La Cour ne se borne donc « pas à rechercher s'il existe une preuve directe de la mise en place d'une opération de surveillance, car pareille preuve est en général difficile – sinon impossible – à apporter » (Cour eur. D.H., 18 mai 2010, n° 26839/05, *Kennedy c. Royaume-Uni*, § 122). Selon cette dernière, la crainte ou menace de surveillance suffit en soi à restreindre la liberté des communications et constitue une ingérence au sens de l'art. 8 de la CEDH (Cour eur. D.H., 6 septembre 1978, *Gerhard Klass e.a. c. Allemagne*, *Série A*., vol. 28, § 41). La Cour estime dès lors qu'il se justifie de déroger à la règle selon laquelle les particuliers n'ont pas le droit de se plaindre d'une loi *in abstracto* afin de « s'assurer que le caractère secret de pareilles mesures ne conduise pas à ce qu'elles soient en pratique inattaquables et qu'elles échappent au contrôle des autorités nationales et de la Cour » (Cour eur. D.H., 18 mai 2010, n° 26839/05, *Kennedy c. Royaume-Uni*, § 124). Cette appréciation large de la qualité de « victime » par la Cour facilite ainsi l'introduction de recours « stratégiques » d'associations de défense des droits de l'homme. Q. EIJKMAN, « Indiscriminate Bulk Data Interception and Group Privacy : Do Human Rights Organisations Retaliate Through Strategic Litigation ? », *Group Privacy*, Philosophical Studies Series, vol. 126, New York, Springer International Publishing, 2017, pp. 123-138.

114 La Cour eur. D.H. apprécie le caractère prévisible d'une telle disposition en tenant compte du fait qu'elle s'exerce en secret. Selon la Cour, la prévisibilité « ne saurait signifier qu'un individu doit se trouver à même d'escompter quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence ». Toutefois, la base légale applicable doit « prévoir en termes suffisamment clairs et détaillés les circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes » et ceci, « d'autant que les procédés techniques utilisables ne cessent de se perfectionner » (Cour eur. D.H., 19 mai 2010, n° 26839/05, *Weber et Saravia c. Allemagne*, § 93).

l'effacement ou la destruction des enregistrements »[115]. Approfondissons certains de ces critères.

A. – *Le champ d'application de la mesure*

Selon la Cour eur. D.H., le champ d'application de la mesure doit être déterminé avec suffisamment de précision d'une part, concernant la nature des infractions susceptibles de donner lieu à un mandat d'interception et d'autre part, vis-à-vis des catégories de personnes susceptibles d'être concernées.

S'agissant des infractions, la Cour eur. D.H. n'exige pas de prévoir une liste exhaustive[116]. La mesure peut, par exemple, viser de manière large « les faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique » et ainsi, conférer aux autorités une « latitude quasi illimitée » lorsqu'il s'agit d'identifier les actes susceptibles de faire procéder à l'interception des communications[117]. La Cour eur. D.H. examine en effet si la marge de manœuvre laissée aux autorités peut être limitée par le biais d'une autorisation judiciaire préalable par exemple[118]. Concernant les personnes susceptibles de faire l'objet d'une mesure de surveillance, il peut s'agir d'un suspect ou d'un prévenu, mais aussi d'un individu susceptible de détenir des informations sur une infraction ou d'autres informations pertinentes pour un dossier pénal[119].

Les mesures comportant un risque de connaître une interception des communications à grande échelle[120] ne semblent pas emporter *ipso facto* la violation de la Convention, la Cour examinant l'ensemble des garanties offertes par la disposition soumise à son contrôle[121] et ce, sans soumettre « les règles gouvernant l'interception de communications individuelles et les dispositifs de surveillance plus généraux à des critères d'accessibilité et de clarté différents »[122]. À titre illustratif, dans l'arrêt *Szabo c. Hongrie*, tout en marquant certaines préoccupations compte tenu du risque d'ouvrir la voie à une « surveillance illimitée d'un grand nombre

115 Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 231.
116 *Ibid.*, § 244.
117 *Ibid.*, § 248. La règlementation visait en effet potentiellement toute « personne susceptible de détenir des informations sur une infraction pénale » mais aussi toute « personne susceptible de détenir des informations pertinentes pour un dossier pénal » en raison de « faits ou activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Fédération de Russie ».
118 Cour eur. D.H. (Gde ch), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 249.
119 *Ibid.*, § 245.
120 Cour eur. D.H., 12 janvier 2016, n° 37138/14, *Szabo et Vissy c. Hongrie*, § 69.
121 *Ibid.*, § 67.
122 Cour eur. D.H., 1er juillet 2008, n° 58243/00, *Liberty e.a. c. Royaume-Uni*, § 28.

de citoyens », la Cour eur. D.H. affirma que le recours à des technologies de pointe y compris le contrôle massif des communications, est une conséquence naturelle eu égard aux nouvelles formes de terrorisme[123]. Faisant référence à son homologue localisée à Luxembourg, la C.J.U.E., elle examina néanmoins le caractère « nécessaire dans une société démocratique » d'un tel dispositif de manière « stricte » : premièrement, de manière générale au regard l'objectif poursuivi en l'occurrence, la sauvegarde des institutions démocratiques, deuxièmement, en particulier, afin d'obtenir des renseignements dans le cadre d'une opération individuelle[124]. Selon certains auteurs, à travers ce double raisonnement, la Cour aurait « marqué un tournant dans sa jurisprudence » considérant « qu'un moyen de surveillance non ciblé doit en lui-même satisfaire le critère de stricte nécessité » limitant ainsi la marge d'appréciation des États quant aux choix entre différentes méthodes de surveillance[125].

B. – *L'autorisation de procéder à l'interception des communications*

Pour déterminer si la procédure d'autorisation est à même de garantir que la surveillance secrète n'est pas ordonnée au hasard, irrégulièrement ou sans examen approprié et convenable, la Cour eur. D.H. prend en compte un certain nombre de facteurs, parmi lesquels, notamment, le service compétent pour autoriser la surveillance, la portée de l'examen qu'il effectue et le contenu de l'autorisation d'interception[126]. Ce service ne doit pas forcément être un service « judiciaire », il doit néanmoins disposer d'une indépendance suffisante à l'égard de l'exécutif[127].

La portée de l'examen revêt une importance particulière dans le cas où le champ d'application de la mesure est large, la latitude laissée aux autorités pouvant être contrebalancée par « une interprétation judiciaire établie de ces termes ou à une pratique consacrée consistant à vérifier au cas par cas s'il existe des raisons suffisantes d'intercepter les communications d'une personne donnée »[128]. À titre illustratif, dans l'arrêt *Roman Zakharov*, la Cour considéra que cet examen doit

123 *Ibid.*, § 68. La disposition visait « la prévention, le suivi et la répression des actes terroristes » ainsi que la collecte de « renseignements nécessaires à la sauvegarde de citoyens en détresse à l'étranger ». Celles-ci ont été considérées comme des indications suffisamment claires sur les circonstances et les conditions dans lesquelles les autorités publiques sont en droit d'avoir recours à une telle mesure. *Ibid.*, § 63.

124 *Ibid.*, §§ 73 et 77.

125 F. DUBUISSON, « La Cour EDH et la surveillance de masse », *R.T.D.H.*, 2016, p. 882. Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*.

126 *Ibid.*, § 257.

127 *Ibid.*, § 258.

128 *Ibid.*, § 249.

permettre de vérifier la présence d'un « soupçon raisonnable » à l'égard de la personne concernée[129], c'est-à-dire de « rechercher s'il existe des indices permettant de la soupçonner de projeter, de commettre ou d'avoir commis des actes délictueux ou d'autres actes susceptibles de donner lieu à des mesures de surveillance secrète, comme par exemple des actes mettant en péril la sécurité nationale »[130]. Dans l'arrêt *Szabo* par contre, la Cour admit la présence d'un « soupçon individuel » à l'encontre d'une personne pour justifier l'interception de ses communications[131]. Cette décision fut vivement critiquée par le Juge Pinto de Albuquerque[132]. Selon ce dernier, en admettant la simple existence d'un « soupçon individuel », la Cour aurait élargi la possibilité de procéder à l'exécution d'un tel dispositif et aurait affaibli le critère retenu par la Grande chambre dans l'arrêt *Roman Zakharov*[133]. *A contrario*, selon certains auteurs, la Cour aurait soumis une pratique de plus en plus répandue des services de renseignements à une critère de nécessité « autonome et plus exigeant » compte tenu du risque pour des personnes non soupçonnées individuellement de connaître une ingérence dans leur vie privée[134]. La Cour eur. D.H. sera sans doute amenée à préciser sa position, celle-ci ayant été saisie de plusieurs recours[135] dont l'affaire *Big Brother Watch* introduite par trois ONG se plaignant de l'interception généralisée des communications véhiculées via les câbles transatlantiques en fibres optiques par le *Government Communications Headquarters* (GCHQ)[136].

On peut espérer une distinction plus claire des critères applicables dans le cadre des interceptions des communications à des fins « stratégiques » exercées par les services de renseignements, de celles exercées dans le cadre de poursuites pénales.

129 *Ibid.*, § 260.
130 *Ibid.*, § 260.
131 Cour eur. D.H., 12 janvier 2016, n° 37138/14, *Szabo et Vissy c. Hongrie*, §§ 71 et 73.
132 Opinion discordante du Juge Pinto de Albuquerque, Cour eur. D.H., 12 janvier 2016, n° 37138/14, *Szabo et Vissy c. Hongrie*.
133 Cour eu. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*.
134 F. DUBUISSON, « La Cour EDH et la surveillance de masse », *op. cit.*, p. 884. Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*.
135 Voyez également l'affaire Cour eur. D.H., n° 62322/14, *Bureau of Investigative Journalism et Alice Ross c. Royaume-Uni*. Cette affaire fait suite à une plainte de journalistes en raison d'une interception de leurs communications téléphoniques et leurs communications par Internet par des organismes gouvernementaux britanniques et notamment par le *Government Communication Headquarters* (service de renseignement électronique) entrainant une ingérence disproportionnée dans le droit des journalistes à la liberté d'expression et dans le droit au respect de la vie privée.
136 Cour eur. D.H., n° 58170/13, *Big Brother Watch et autres c. Royaume-Uni*, communiquée au Gouvernement défendeur le 7 janvier 2014.

C. – *La conservation et la destruction des données recueillies*

La Cour admet une retranscription partielle des données interceptées pour autant que l'intéressé se voit offrir la possibilité d'accéder aux enregistrements et d'en contester la véracité[137]. En outre, la période de conservation des données doit être justifiée et le moment de leur destruction doit être précisé notamment si elles sont conservées à l'issue du procès[138]. Enfin, les données ne présentant aucun lien avec l'objectif poursuivi doivent en principe être détruites « sur-le-champ »[139].

D. – *La notification a posteriori et le contrôle effectif par un organe indépendant*

La notification *a posteriori*, c'est-à-dire, l'information fournie à la personne une fois la mesure levée, a des conséquences sur l'effectivité du recours susceptible d'être exercé par celle-ci[140]. Les personnes concernées ne pourraient en effet mettre en cause une mesure prise à leur insu sans en avoir été averties, à moins de pouvoir soupçonner que leurs communications ont fait l'objet d'interceptions[141]. Selon la Cour eur. D.H., cette notification est certes souhaitable mais ne saurait être imposée dans tous les cas au risque de nuire à l'efficacité du dispositif[142]. Il est en revanche préconisé, d'après celle-ci, « d'aviser la personne concernée après la levée des mesures de surveillance dès que la notification peut être donnée sans compromettre le but de la restriction »[143].

Le contrôle exercé sur la mesure peut être mis en œuvre à trois stades « lorsqu'on l'ordonne, pendant qu'on la mène ou après qu'elle a

137 Cour eur. D.H., 26 avril 2007, n° 71525/01, *Dumitru Popescu c. Roumanie (n° 2)*, § 78.

138 Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 256.

139 Selon la Cour, une conservation automatique durant 6 mois de données manifestement dénuées d'intérêt n'est pas justifiée au regard de l'art. 8, § 2, de la Convention (Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 255).

140 Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 234.

141 *Ibid.*

142 En effet, « pareille notification risquerait de contribuer à révéler les méthodes de travail des services de renseignements, leurs champs d'observation et même, le cas échéant, l'identité de leurs agents » (Cour eur. D.H., 6 septembre 1978, *Gerhard Klass e.a. c. Allemagne*, *Série A*., vol. 28, § 58). Dès lors « l'absence de notification *a posteriori* aux personnes touchées par des mesures de surveillance secrète, dès la levée de celles-ci, ne saurait en soi justifier la conclusion que l'ingérence n'était pas "nécessaire dans une société démocratique" » (Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 287). La Cour a donc estimé que constituait une garantie suffisante une disposition n'imposant pas de notification mais permettant à toute personne soupçonnant avoir fait l'objet d'une telle mesure de saisir la commission des pouvoirs d'enquête (Cour eur. D.H., 18 mai 2010, n° 26839/05, *Kennedy c. Royaume-Uni*, § 167).

143 Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 287.

cessé »[144]. Dans le cas d'une mesure de surveillance secrète, les deux premières phases sont par essence inexistantes ainsi que le contrôle qui l'accompagne. Compte tenu de cette particularité, la Cour eur. D.H. recommande un contrôle en dernier ressort par le pouvoir judiciaire, celui-ci offrant « les meilleures garanties d'indépendance, d'impartialité et de procédure régulière »[145]. Un contrôle par un organe non judiciaire peut s'avérer compatible avec la Convention sous réserve de l'indépendance de ce dernier vis-à-vis des autorités procédant à la surveillance et de ses pouvoirs qui doivent lui permettre d'exercer un contrôle efficace et permanent[146].

L'indépendance de cet organe est examinée à la lumière de différents facteurs tels le mode de désignation[147] et le statut juridique des membres de l'organe de contrôle[148]. À titre illustratif, ne saurait être considéré comme suffisamment indépendant, un procureur général ainsi que les procureurs de rang inférieur[149], d'autant lorsqu'il existe un mélange de fonctions au sein du parquet où le même service approuve les demandes d'interception puis contrôle la mise en œuvre de l'opération[150]. D'un point de vue pratique, l'organe de contrôle doit pouvoir accéder à tous les documents pertinents y compris les informations confidentielles et être en mesure d'ordonner à toute personne participant à l'interception de fournir les informations souhaitées[151]. Il doit également disposer d'un certain pouvoir en cas d'infractions, par exemple, être en mesure d'exiger la destruction des éléments interceptés de manière illégale[152]. Enfin, la Cour examine si les activités de l'organe de contrôle sont soumises à un droit de regard du public lui permettant de constater l'effectivité concrète du système de contrôle[153].

144 Cour eur. D.H., 6 septembre 1978, *Gerhard Klass e.a. c. Allemagne*, *Série A*., vol. 28, § 55.

145 *Ibid.* À ce propos, voy. M. GIANCLAUDIO et P. DE HERT, « European Human Rights, Criminal Surveillance, and Intelligence Surveillance : Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges », in *The Cambridge Handbook of Surveillance Law* (D. GRAY et S. HENDERSON), Cambridge, Cambridge University Press, 2017, pp. 509-532.

146 Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 278.

147 Ainsi, la Cour a considéré que rencontraient de telles exigences un organe composé de parlementaires ou de personnes possédant les qualifications requises pour accéder à la magistrature et nommées soit par le parlement soit par le premier ministre. Cour eur. D.H., *Weber et Saravia c. Allemagne*, préc., § 117. Par contre, ne saurait être considéré comme suffisamment indépendant un ministre de l'Intérieur nommé par le pouvoir politique et membre de l'exécutif, par ailleurs impliqué dans la commande de moyens de surveillance. Cour eur. D.H., 28 juin 2007, n° 62540, *Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev*, §§ 85 et 87.

148 Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 275.

149 Cour eur. D.H., 10 février 2009, n° 25198/02, *Iordachi et autres c. Moldavie*, § 47.

150 Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 280.

151 *Ibid.*, § 281.

152 Cour eur. D.H., 18 mai 2010, n° 26839/05, *Kennedy c. Royaume-Uni*, § 168.

153 Cour eur. D.H. (Gde ch.), 4 décembre 2015, n° 47143/06, *Roman Zakharov c. Russie*, § 283.

VIII. Conclusions

La volonté de tirer certaines lignes de forces des enseignements de la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme s'avère être un exercice délicat compte tenu de l'absence d'harmonisation des procédure pénales au sein des États membres.

En cas d'ingérence dans l'exercice du droit à la vie privée, la Cour eur. D.H. et la C.J.U.E. portent une attention particulière à l'existence de garanties suffisantes contre les abus. Certaines de celles-ci sont devenues des « classiques » reprises par le Groupe de l'Article 29 sous l'intitulé « *European Essential Guarantees* ». Ainsi, (a) tout traitement de données à caractère personnel devrait être basé sur des règles claires précises et accessibles ; (b) la nécessité et la proportionnalité des objectifs légitimes poursuivis devraient être démontrées ; (c) la mesure devrait être soumise au contrôle d'un organisme indépendant ; (d) des recours effectifs devraient être offerts aux personnes concernées[154].

Si ces conditions permettent de limiter l'ingérence au « strict nécessaire », on peut regretter l'adoption de mesures de plus en plus invasives à des fins de « sécurité nationale » sans un examen scrupuleux de l'objectif effectivement poursuivi. Comme le souligne le Groupe de l'Article 29 au sujet de la surveillance des communications électroniques, « il conviendrait de déterminer dans quelle mesure une ingérence fondée sur la sécurité nationale demeure le reflet de la réalité, maintenant qu'il apparaît que le travail des services de renseignement est plus que jamais interconnecté avec celui des autorités répressives et qu'il poursuit plusieurs objectifs différents »[155].

En outre, en offrant des garanties procédurales suffisantes et un cadre de plus en plus précis, on prive parallèlement l'individu de la facette négative du droit au respect de la vie privée, à savoir, le droit à la non immixtion des pouvoirs publics dans son intimité. Cette procéduralisation de l'article 8 de la CEDH et des articles 7 et 8 de la Charte aboutit paradoxalement à un affaiblissement du droit à la vie privée et à la protection des données à caractère personnel.

154 Groupe de l'Article 29, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 avril 2016.

155 Groupe de l'Article 29, avis 04/2014 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale, 10 avril 2014.